Remarks

Claims 1, 10, 11 and 14 have been amended to correct the improper numbering of the subparagraphs due to a computer problem.

Wrong drawings were submitted with this specification due to a clerical error. The correct set of drawings for Figures 1-6 are submitted herewith.

No new matter has been added.

Respectfully,

G Fre

Gordon Freedman, Reg. No. 41,553

Freedman & Associates
117 Centrepointe Drive, Suite 350
Nepean, Ontario
K2G 5X3 Canada

Tel: (613) 274-7272
Fax: (613) 274-7414
Email: gordon@ipatent4u.com

ATTACHMENT A

Clean Replacement Claims and Drawings

Please replace the following claims with the following clean claims as follows:

Claims 1, 10, 11 and 14.

A1

1. A method for transferring a first electronic key between a key provider system and a second other system via an information network comprising the steps of:

a) encrypting the first electronic key using a first encryption key of the key provider;

b) providing within the second other system a first secure module having a second encryption key within a read-only memory circuit thereof and provided with the first secure module, the second encryption key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second encryption key is other than modifiable and other than accessible outside of the module;

c) transferring the encrypted first electronic key from the key provider system to the second other system via the information network;

d) providing the encrypted first electronic key to the processor internal to the first secure module of the second other system; and,

e) executing program code on the processor internal to the first secure module to decrypt the encrypted first electronic key using the second encryption key stored within the read-only memory circuit of the first secure module and to store the decrypted first electronic key internally within a secure key memory location of the first secure module.

A2 cont

10. A method for transferring a first electronic key between a key provider system and a second other system via an information network comprising the steps of:

a) encrypting the first electronic key using a first encryption key of the key provider;

b) providing within the second other system a first secure module having second and third encryption keys within a memory circuit thereof, the second and third encryption keys accessible only by program code being executed on a processor internal to the first secure module for decrypting encrypted electronic keys and for storing the decrypted electronic keys within a memory circuit of the first secure module, and wherein the second and third encryption keys are other than accessible outside of the module;

c) transferring the encrypted first electronic key from the key provider system to the second other system via the information network;

d) providing the encrypted first electronic key to the processor internal to the first secure module of the second other system; and,

e) executing program code on the processor internal to the first secure module to decrypt the encrypted first electronic key using the second encryption key stored within the memory circuit of the first secure module and to store the decrypted first electronic key internally within a secure key memory location of the first secure module.

A2 Cncld.

11. A method for transferring a first electronic key between a key provider system and a second other system via an information network according to claim 10 comprising the steps of:

f) encrypting a fourth encryption key using one of the third encryption key and a key corresponding to the third encryption key;

g) transferring the encrypted fourth encryption key from the key provider system to the second other system via the information network;

h) providing the encrypted fourth encryption key to the processor internal to the first secure module of the second other system; and,

i) executing program code on the processor internal to the first secure module to decrypt the encrypted fourth encryption key using the third encryption key stored within the memory circuit of the first secure module and to store the decrypted fourth encryption key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second encryption key was stored.

A3 Cnt

14. The method according to claim 11 wherein the step of storing the decrypted fourth encryption key comprises the steps of:

i1) erasing the second encryption key from a first storage area of the memory circuit; and,

i2) storing the decrypted fourth encryption key within approximately the same first storage area of the same memory circuit.

N.E. *Please replace Figures 1-6 currently on file with the following correct Figures 1-6 as follows.*

ATTACHMENT B

Marked Up Version of the Amended Claims

A marked up copy of the amended Claims is provided as follows:

Claims 1, 10, 11 and 14

1. A method for transferring a first electronic key between a key provider system and a second other system via an information network comprising the steps of:

a)[f)] encrypting the first electronic key using a first encryption key of the key provider;

b)[g)] providing within the second other system a first secure module having a second encryption key within a read-only memory circuit thereof and provided with the first secure module, the second encryption key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second encryption key is other than modifiable and other than accessible outside of the module;

c)[h)] transferring the encrypted first electronic key from the key provider system to the second other system via the information network;

d)[i)] providing the encrypted first electronic key to the processor internal to the first secure module of the second other system; and,

e)[j)] executing program code on the processor internal to the first secure module to decrypt the encrypted first electronic key using the second encryption key stored within the read-only memory circuit of the first secure module and to store the decrypted first electronic key internally within a secure key memory location of the first secure module.

10. A method for transferring a first electronic key between a key provider system and a second other system via an information network comprising the steps of:

a) encrypting the first electronic key using a first encryption key of the key provider;

b)[g)] providing within the second other system a first secure module having second and third encryption keys within a memory circuit thereof, the second and third encryption keys accessible only by program code being executed on a processor internal to the first secure module for decrypting encrypted electronic keys and for storing the decrypted electronic keys within a memory circuit of the first secure module, and wherein the second and third encryption keys are other than accessible outside of the module;

c)[h)] transferring the encrypted first electronic key from the key provider system to the second other system via the information network;

d)[i)] providing the encrypted first electronic key to the processor internal to the first secure module of the second other system; and,

e)[j)] executing program code on the processor internal to the first secure module to decrypt the encrypted first electronic key using the second encryption key stored within the memory circuit of the first secure module and to store the decrypted first electronic key internally within a secure key memory location of the first secure module.

11. A method for transferring a first electronic key between a key provider system and a second other system via an information network according to claim 10 comprising the steps of:

f)[k)] encrypting a fourth encryption key using one of the third encryption key and a key corresponding to the third encryption key;

g)[l)] transferring the encrypted fourth encryption key from the key provider system to the second other system via the information network;

h)[m)] providing the encrypted fourth encryption key to the processor internal to the first secure module of the second other system; and,

i)[n)] executing program code on the processor internal to the first secure module to decrypt the encrypted fourth encryption key using the third encryption key stored within the memory circuit of the first secure module and to store the decrypted fourth encryption key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second encryption key was stored.

14. The method according to claim 11 wherein the step of storing the decrypted fourth encryption key comprises the steps of:

i1)[f1)] erasing the second encryption key from a first storage area of the memory circuit; and,

i2)[f2)] storing the decrypted fourth encryption key within approximately the same first storage area of the same memory circuit.

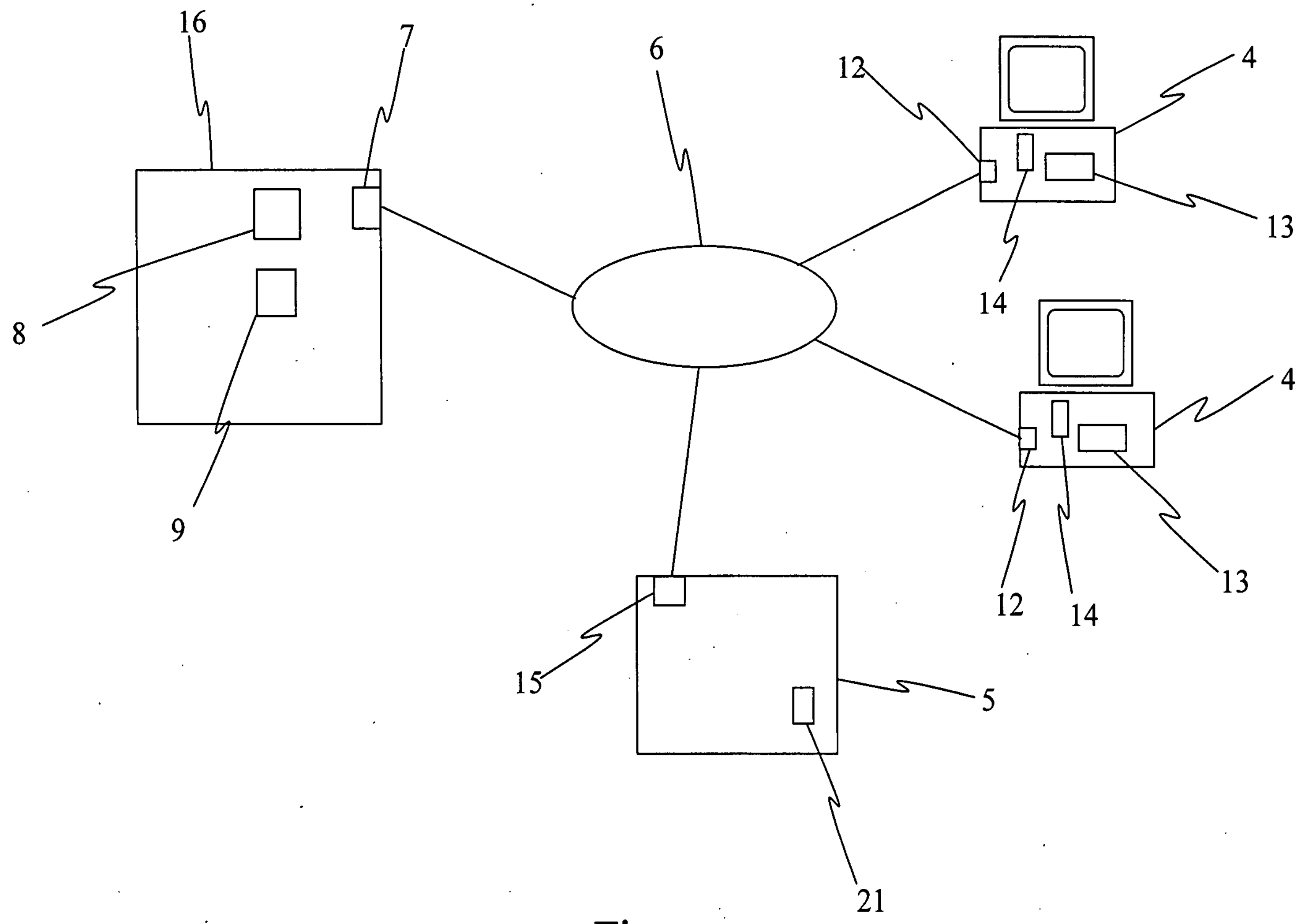

Figure 1
(Prior art)

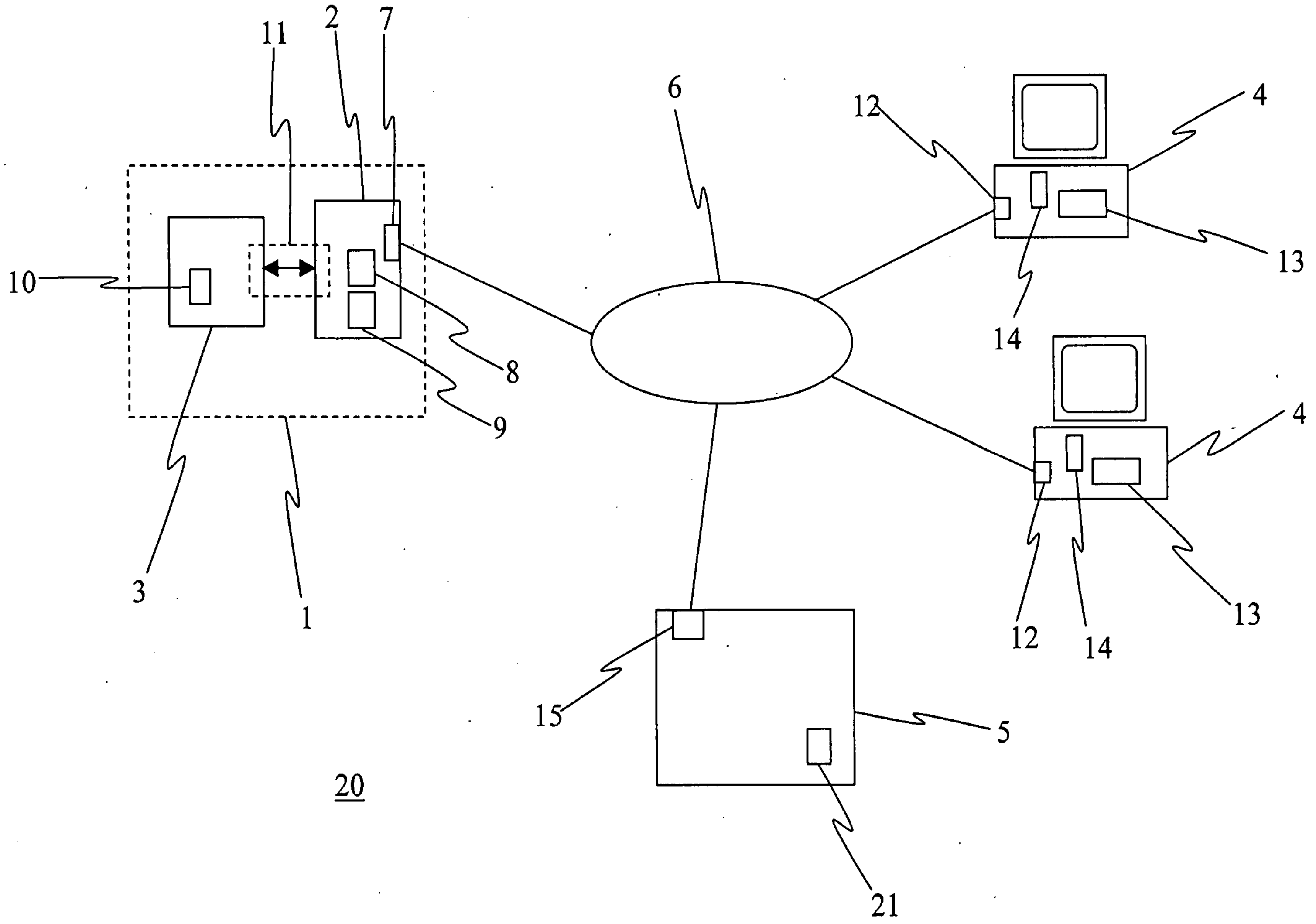

Figure 2

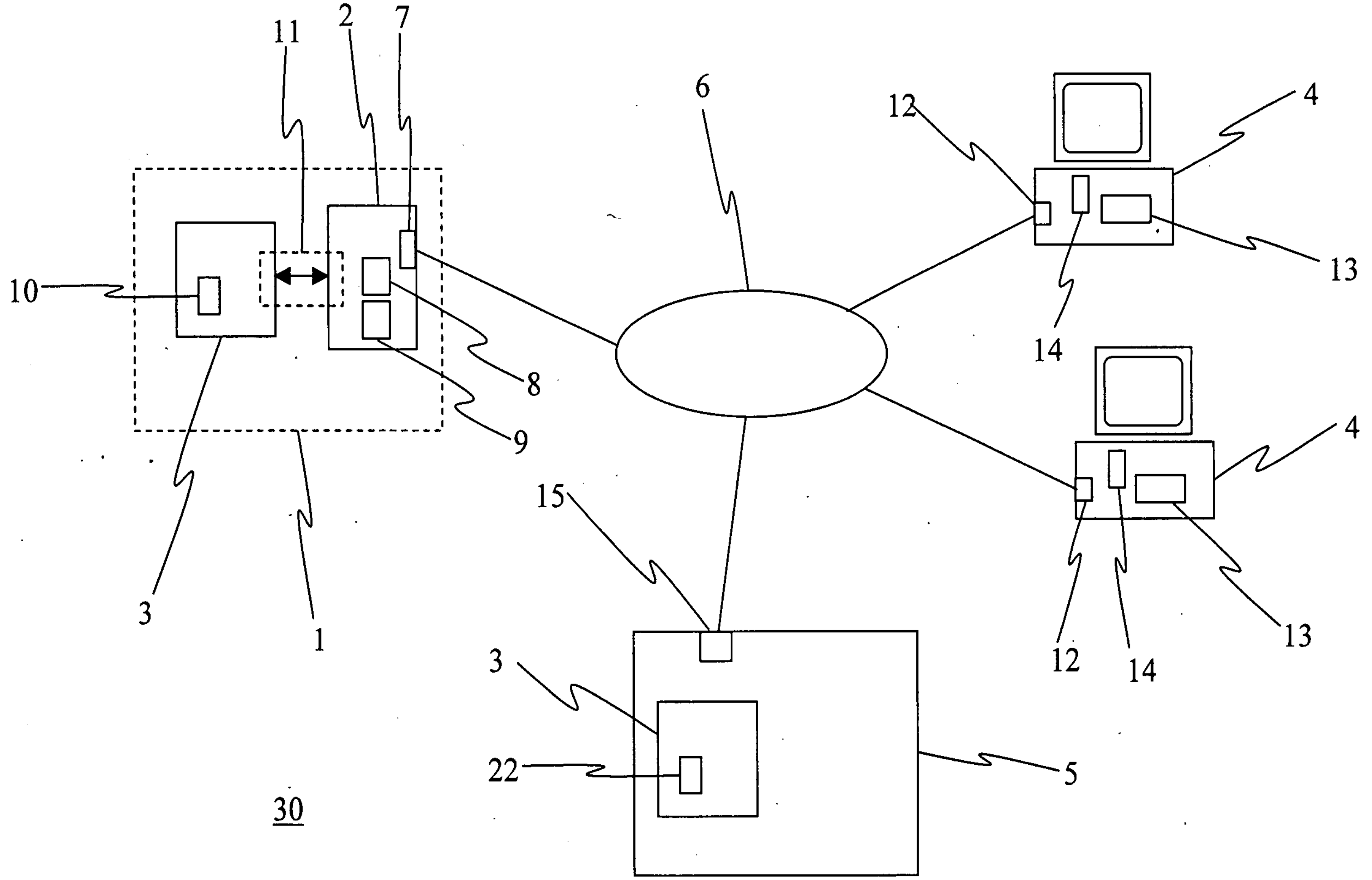

Figure 3

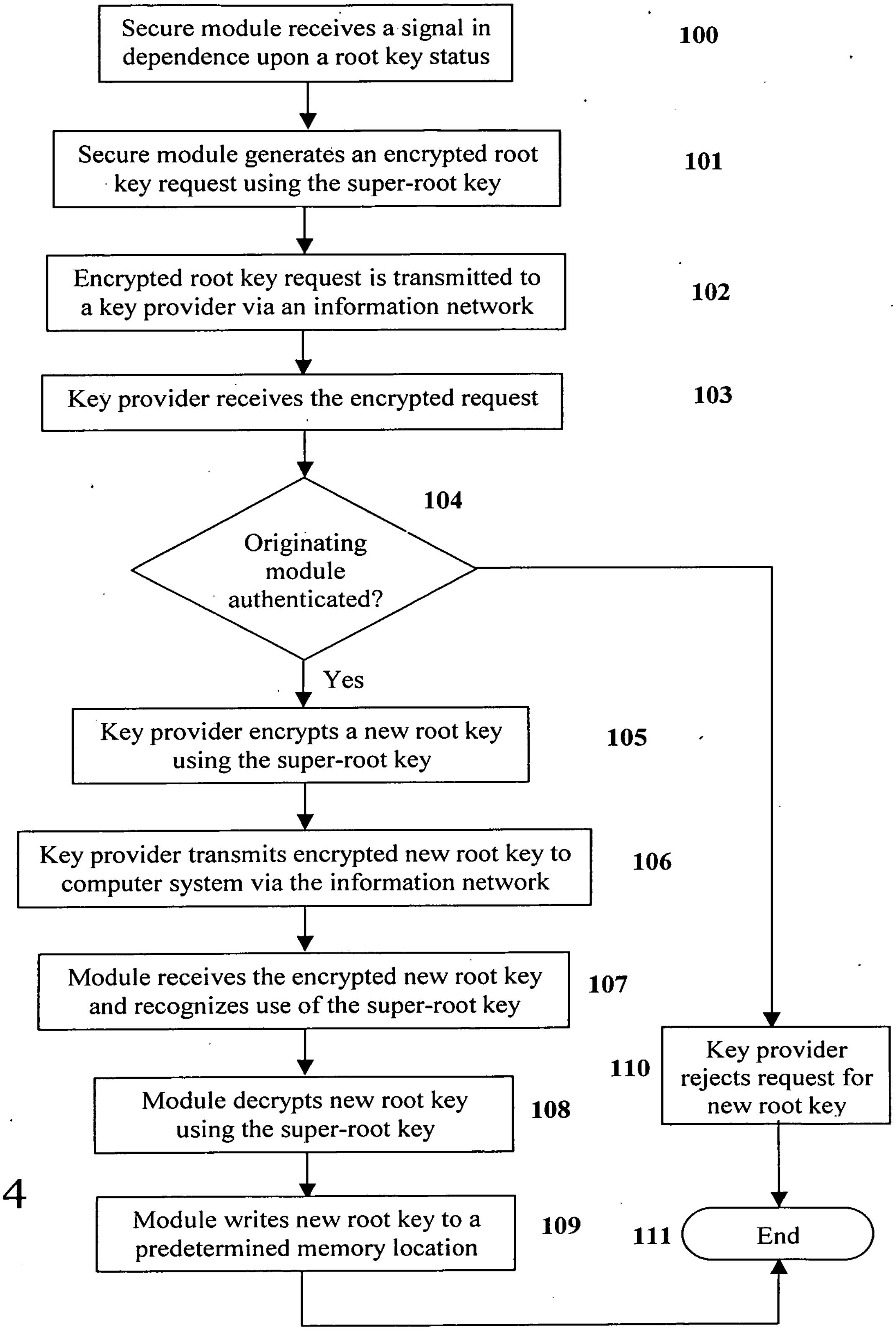
Secure module receives a signal in dependence upon a root key status
100
Secure module generates an encrypted root key request using the super-root key
101
Encrypted root key request is transmitted to a key provider via an information network
102
Key provider receives the encrypted request
103
Originating module authenticated?
104
Yes
Key provider encrypts a new root key using the super-root key
105
Key provider transmits encrypted new root key to computer system via the information network
106
Module receives the encrypted new root key and recognizes use of the super-root key
107
Module decrypts new root key using the super-root key
108
Module writes new root key to a predetermined memory location
109
110
Key provider rejects request for new root key
111
End

Figure 4

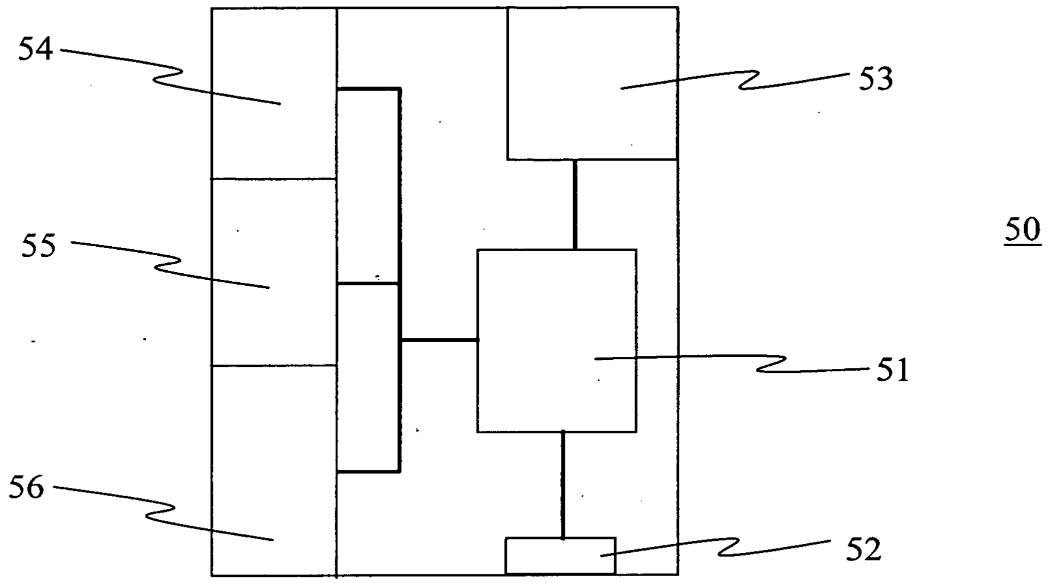

Figure 5

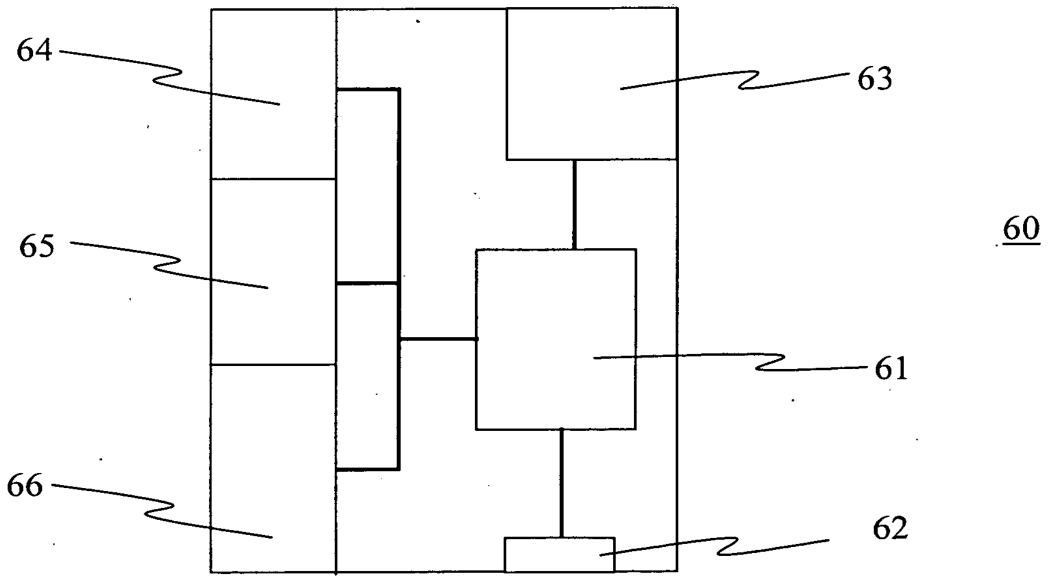

Figure 6